

WHAT IS CLAIMED IS

1. A method for testing an integrated circuit containing hardware and/or software parts having a confidential nature, using a tester, wherein this method comprises the steps of :

- in said integrated circuit:
  - 5 generating a random number,
  - ciphering this random number using a key stored in said integrated circuit via a ciphering algorithm to obtain a first password, and
  - sending the random number to said tester,
- and, in said tester:
  - 10 ciphering in parallel said random number received using a key identical to that used in said integrated circuit via an identical ciphering algorithm to that implemented in said integrated circuit, to generate a second password, and
  - sending said second password from the tester to said integrated circuit,
- then, in said integrated circuit,
  - 15 comparing said first and second passwords,
  - freeing a test path leading from said tester to said parts of a confidential nature, only if the comparison establishes a match between said first and second passwords, and
  - effecting the test of said elements of a confidential nature.

- 20 2. A method according to claim 1, wherein it also comprises the steps of :
- in said integrated circuit:
    - ciphering said random number using said key stored in the integrated circuit via said ciphering algorithm to obtain a third password;
    - sending said third password to said tester;

25 and

- in said tester:
  - ciphering said random number received using said key stored in said tester via said ciphering algorithm to obtain a fourth password;
  - comparing said third and fourth passwords; and
  - 30 authorising the ciphering of said second password via said tester only if there is a match between said third and fourth passwords.

3. A method according to claim 1, wherein it also comprises the steps of :
- in said integrated circuit:
    - ciphering said random number using said key stored in the integrated circuit
    - 35 via said ciphering algorithm to obtain a third password;

- in said tester:

comprising the random number received from said integrated circuit to said calculated random number, and

10           4. A method according to claims 2 or 3, wherein the ciphering of said third and/or fourth passwords is made on the basis of a different number of clock strokes than that used for ciphering said first and second passwords.

6. A method according to claim 1, wherein it comprises the steps of, upon manufacturing said integrated circuit, storing a predetermined value of said cipher key, and during execution of said test procedure using said tester, sending to said integrated circuit, a cipher key value, checking whether said cipher key sent has the predetermined value stored in said integrated circuit, commanding said key sent to be stored in said integrated circuit in case an inequality is observed during said check and blocking in such case the storage in said circuit of any other cipher key.

- a random number generator;
- means for storing a cipher key;
- processing means for calculating a first password from said key and a generated random number, using a cipher algorithm;

8. An integrated circuit according to claim 7, wherein it includes means for storing said first calculated password, said storage means being placed before the

9. An integrated circuit according to claim 7, wherein the means for storing the cipher key are an EEPROM memory which also includes a redundancy unit check.

11. A tester for integrated circuits including hardware and/or software parts having a confidential nature, this tester including means for effecting a proper working test of said hardware and/or software parts to route the corresponding data to said circuit, wherein it includes:

12. A tester according to claim 11, wherein said processing means are also arranged to calculate, using a cipher algorithm, a fourth password from said cipher key and from the received random number;

13. A tester according to claim 11, wherein:

35 wherein it also includes comparison means for checking the match between  
said received random number and said calculated random number, said processing

means only being authorised to calculate said second password if the comparison means observe a predetermined match between said random numbers.

TOGETHER WITH